DRAFT: 5/6/2010

Framing

- The Policy Committee has endorsed a set of meaningful use criteria that require the exchange of data with other providers, with patients, to public health agencies, and, to a limited extent, with payers (for insurance eligibility checks). The expectation is that subsequent stages of meaningful use will likely require greater health information exchange.

- ONC is seeding a number of health information exchange activities, including NHIN Direct, direct funding states to create health information exchange infrastructure, and regional initiatives, in order to support current and future meaningful use requirements. All of these initiatives must have at an early stage a stable privacy framework that can set expectations early and support the evolution to a broader range of services involving potentially greater sharing and distributed use of health information.

- The work to establish standards for exchange – particularly for NHIN Direct – is proceeding rapidly, but to date this work has been uninformed by a clear set of policy expectations and requirements. There is urgent work to be done on technical elements of NHIN Direct, including the specification of standards for the kinds of health information sharing that would support meaningful use.

- But technical standards and technology approaches for information sharing always are based on established or assumed use cases and policy addressing what information is shared, how it is accessed and where it is stored. Thus, in the absence of specific policy the selection of standards and technical approaches inevitably create policy *de facto* -but without a full discussion of those embedded policy assumptions. Privacy and security policies should be established before, or at least be established in tandem with, technical standards. If the policy requirements are not clearly set at the start of these activities, it will be difficult to impossible to retrofit technology later – in terms of both impact to lives and financial costs.

- Standards (for security or for health information generally) are not a substitute for clear policies that are essential to reassure healthcare professionals and consumers that information exchange can improve health outcomes without expressly or implicitly opening the door to inappropriate disclosures or uses of information. Appropriate information flows are essential to improving both individual and population health – but clear, unambiguous policies, and supporting technology, are needed to enable these information flows without (intentionally or unintentionally) exposing that information to unnecessary risk.

- Current law provides a baseline set of requirements– but doesn't provide adequate guidance or answer the important questions posed by the new exchange environment we are trying to create. If we fail to act, the weaknesses in current law will only be exploited by the greater data sharing contemplated by meaningful use.

- ONC issued a Nationwide Privacy and Security Framework in December 2008 that established a set of principles to govern health information exchange. These principles are guideposts – but principles alone are not a policy framework because they do not define the more specific policies and practices needed to implement them. Principles are meant to set high level aspirations - but they are only useful if translated into policies, practices, and technology solutions that specifically implement them in a comprehensive manner.

- The time has come to set forth more specific policies to govern health information exchange – early in the evolution of NHIN Direct and exchange through a local, state, regional or national HIE. The Workgroup began this discussion a couple of months ago looking specifically at the issue of the role of consent in health information exchange. But information policies are never effectively created in isolation. Rather, they must be created within a framework of complementary protections, both policy and technical, that work together to protect personal information.

Recommendations

- We need a complete *policy and technology* framework that implements the principles in the Nationwide Privacy and Security Framework, that includes the specific policies and practices to govern digital health information exchange, and that sets expectations for what the technology must achieve. Such a framework should assume existing law and fill gaps, clarify the policies that technology and operational practices must enforce, be applicable to all entities that are exposed to health information, and be established through a combination of policy requirements, policy-specific technical requirements, and industry best practices.

- We must begin this work immediately, and it should proceed joined at the hip with the work currently being done to establish standards for NHIN Direct and requirements for state HIE and extension center grants. FACA bodies have an important role to play in establishing this framework, but we will need more support in order to make more specific recommendations and meet strict timelines.

- Much of the focus of privacy conversations (both nationally and at the state level) is on the role of consumer consent, and consumer choice or consent plays an important role in a comprehensive policy and technology framework. But consent should not be the driver in setting privacy policy, because it essentially shifts the burden of protecting privacy to the individual who is left to choose whether data use and exchange within a particular model is trustworthy (a model the individual is not likely to understand). To truly build trust in health information exchange, we must do the hard work of setting terms and conditions of usage and exchange (both in terms of policy and technology). The role that effective, well informed consent can play should be considered within that context.

- We have in place a set of laws that currently provide some context for "point-to-point" exchange of data, particularly for Stage 1 of Meaningful Use, where there is no "intermediary" in the middle with access to the data. [Note: the term "intermediary" refers to entities in the middle that access some data – at any layer of the technology stack that is required to share information securely- in order to perform a function that facilitates exchange or provides a a "value added" service.] This type of point-to-point exchange without an intermediary feels most like the type of exchange that occurs today. Current law was built on the assumptions in this model, and it is largely consistent with patient expectations. Consequently, in this narrow setting, we don't believe that any additional patient consent requirements are needed beyond what is already set forth in current law.

- However, even simple exchange is likely to depend on an intermediary providing some type of service that involves access to data, creating additional exposures and vulnerabilities. (For example, the HIPAA Security Rule addresses clearinghouses, which may help covered entities bring their HIPAA transactions into compliance with standards.) There need to be clear enforceable policies and technology requirements for all participants in health information exchange as well as for intermediaries of several types who may have varying levels of access to information. Such policies should include:
    - constraints on collection, access and disclosure of identifiable data;
    - constraints on data retention and re-use; and
    - minimal security requirements.

  We should consider the role of consent in direct exchange using intermediaries – but should do so only as part of a broader discussion about the policy and technology framework.

<u>Further Discussion:</u>

- Examples of just some of the questions that should be addressed in developing this framework, beginning with direct exchange:

    - For intermediaries providing basic levels of services like identity management, routing, or provider directory services, what access to data in the message envelope is needed to perform the service(s)? Is there any justification for allowing access to unencrypted data in the payload (message content)?
    - How long should such data collected be retained? What happens to the data after the service has been provided?

  - What, if any, reuses of such data should be permitted?
  - What technological requirements are needed to support policies around data access, use, disclosure, and retention (even on media that are reused)?
  - What other services are intermediaries likely to provide and what specific policies are needed to secure and maintain trust?
  - Who can access patient information directly from intermediaries and for what purposes?
  - What about further use and disclosure of de-identified information?
  - What did we learn from the Health Information Security and Privacy Collaborative (HISPC) work that can be instructive here?

- We also need to contemplate the broad range of exchange architectures that could exist (and whether they should exist), and how should the privacy and security principles be translated into policies and technology requirements needed to build trust in a particular type of exchange. The Workgroup has spent much of its time talking about direct or "vetted" exchange, where information is shared directly between two covered entities. But other models, such as those that involve the creation of large databases of individually identifiable health information that can be mined or queried , while allowable within current law, may raise concerns with respect to patient expectations. What policies and technical requirements are needed to build trust in these models, and what additional role should consumer choice play in building public trust?

- Enforcement of policies and requirements is also critical. These intermediaries are likely to be business associates under HIPAA. But unfortunately the business associate rules as currently interpreted do not provide sufficient specificity to serve as an effective policy framework to govern the activities of intermediaries in exchange. Among the concerns raised by workgroup members are the following:

  -business associate rules are either too lax or have been interpreted to allow chains of business associates to use information to serve their own or others' business needs (vs. merely serving the needs of the covered entity whose data they possess).

  -an increase in the access to and use of de-identified data in an environment with insufficient protections against (and penalties for) inappropriate re-identification.

  -potential access to intermediary data by entities not currently governed by federal (or sometimes state) health privacy rules.

  -data moving through chains of subcontractors with uncertain accountability.

- Even with more specific rules, it is unclear whether business associate agreements provide an effective enforcement tool.

  -Currently, BA agreements are not required to include specific provisions limiting access to information. They have customarily been largely form documents that require compliance with HIPAA.

  -The balance of power may more likely be tipped toward the HIE/intermediary than the covered entity (for example, to take advantage of using the network to exchange data for MU, the covered entity may be required to agree to less desirable terms with respect to data use and re-use).

  -If it is possible to have more clear rules on business associate agreements, at least for intermediaries (for example, require certain provisions), enforcing these policies through BAAs has the advantage of piggybacking on substantial penalties for failure to comply.

  -However, this is only effective to govern two levels of exchange – from covered entity to one business associate; it does not effectively govern beyond those levels – such as a business associate to its sub-contractor.

- If the business associate rules are not an effective mechanism for setting policy and technology requirements for intermediaries, we may need to enforce through other governance mechanisms.

  -Is governing and overseeing these policies and requirements just a federal responsibility or do states/communities have a role?

  -Do we have sufficient existing authority to implement these policies in a consistent manner? (critical for interoperability)